

# Packet Capture

Cihazımızda anlık capture almak isteyebiliriz bunu için

Capture filterlerinin konfigürasyonu için ;

```
Lab(NOLICENSE)#debug packet l3-protocol ip 192.168.10.20 count 50
```

Capture başlatmak için

```
Lab(NOLICENSE)#debug monitor
```

Bitirmek için

```
Lab(NOLICENSE)#no debug monitor
```

Örnek çıktı ;

```
Lab(NOLICENSE)#debug packet l3-protocol ip 192.168.10.20 count 50
Lab(NOLICENSE)#deb
Lab(NOLICENSE)#debug mo
Lab(NOLICENSE)#debug monitor
Wait for debug output, enter <ctrl c> to exit
@4310020895 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 icmp echo req seq=12011
@4310020895 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3070 > 80 S dbc5606:0(0) <mwt, m=1460,w=7>
@4310020895 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 icmp echo req seq=12010
@4310020900 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3070 > 80 A dbc5607:191a8ef(0)
@4310020922 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3070 > 80 FA dbc5607:191a8ef(0)
@4310020924 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3070 > 80 A dbc5608:191a8f0(0)
@4310020898 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 icmp echo rsp seq=12011
@4310020898 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 tcp 80 > 3070 SA 191a8ee:dbc5607(0) <mwt, m=1460,w=7>
@4310020898 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 icmp echo rsp seq=12010
@4310020922 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 tcp 80 > 3070 FA 191a8ef:dbc5608(0)
@4310022154 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 icmp echo req seq=12012
@4310022154 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3074 > 80 S 6efe75c9:0(0) <mwt, m=1460,w=7>
@4310022154 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 icmp echo req seq=12011
@4310022156 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3074 > 80 A 6efe75ca:6167b9ed(0)
@4310022181 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3074 > 80 FA 6efe75ca:6167b9ed(0)
@4310022182 o( 2, 0)> ip 192.168.10.10 > 192.168.10.20 tcp 3074 > 80 A 6efe75cb:6167b9ee(0)
@4310022154 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 icmp echo rsp seq=12012
@4310022154 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 tcp 80 > 3074 SA 6167b9ec:6efe75ca(0) <mwt, m=1460,w=7>
@4310022154 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 icmp echo rsp seq=12011
@4310022181 i( 2, 1)> ip 192.168.10.20 > 192.168.10.10 tcp 80 > 3074 FA 6167b9ed:6efe75cb(0)
@4310022299 o( 2, 0)> ip 192.168.10.53 > 192.168.10.20 tcp 2054 > 80 S 92df81a0:0(0) <mwt, m=1460,w=2>
@4310022299 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 SA b58117b3:92df81a1(0) <mwt, m=1460,w=7>
@4310022299 o( 2, 0)> ip 192.168.10.53 > 192.168.10.20 tcp 2054 > 80 PA 92df81a1:b58117b4(378)
@4310022300 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 A b58117b4:92df831b(0)
@4310022300 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 A b58117b4:92df831b(1448)
@4310022300 o( 1, 0)> ip 5.5.5.5 > 172.16.50.10 tcp 80 > 47234 PA a03f677:a97891e5(1448)
@4310022300 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 A b5811d5c:92df831b(1448)
@4310022300 o( 2, 0)> ip 192.168.10.53 > 192.168.10.20 tcp 2054 > 80 A 92df831b:b5812304(0)
@4310022300 o( 1, 0)> ip 5.5.5.5 > 172.16.50.10 tcp 80 > 47234 PA a03fc1f:a97891e5(1448)
@4310022300 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 PA b5812304:92df831b(581)
@4310022300 o( 1, 0)> ip 5.5.5.5 > 172.16.50.10 tcp 80 > 47234 PA a0401c7:a97891e5(581)
@4310022311 i( 1, 1)> ip 172.16.50.10 > 5.5.5.5 tcp 47234 > 80 A a97891e5:a03fc1f(0)
@4310022311 i( 1, 1)> ip 172.16.50.10 > 5.5.5.5 tcp 47234 > 80 A a97891e5:a0401c7(0)
@4310022311 i( 1, 1)> ip 172.16.50.10 > 5.5.5.5 tcp 47234 > 80 A a97891e5:a04040c(0)
@4310022314 o( 2, 0)> ip 192.168.10.53 > 192.168.10.20 tcp 2054 > 80 A 92df831b:b5812549(0)
@4310022329 o( 2, 0)> ip 192.168.10.54 > 192.168.10.20 tcp 2054 > 80 S da6ada0d:0(0) <mwt, m=1460,w=2>
@4310022329 i( 2, 1)> ip 192.168.10.20 > 192.168.10.54 tcp 80 > 2054 SA 3a4be2f6:da6ada0e(0) <mwt, m=1460,w=7>
@4310022329 o( 2, 0)> ip 192.168.10.54 > 192.168.10.20 tcp 2054 > 80 PA da6ada0e:3a4be2f7(421)
@4310022329 i( 2, 1)> ip 192.168.10.20 > 192.168.10.54 tcp 80 > 2054 A 3a4be2f7:da6adbb3(0)
@4310022329 i( 2, 1)> ip 192.168.10.20 > 192.168.10.54 tcp 80 > 2054 PA 3a4be2f7:da6adbb3(181)
@4310022329 o( 1, 0)> ip 5.5.5.5 > 172.16.50.10 tcp 80 > 47236 PA b30ad077:6120d37c(181)
@4310022341 i( 1, 1)> ip 172.16.50.10 > 5.5.5.5 tcp 47236 > 80 A 6120d37c:b30ad12c(0)
@4310022343 o( 2, 0)> ip 192.168.10.54 > 192.168.10.20 tcp 2054 > 80 A da6adbb3:3a4be3ac(0)
@4310022559 i( 1, 1)> ip 172.16.50.10 > 5.5.5.5 tcp 47234 > 80 PA a97891e5:a04040c(352)
@4310022559 o( 2, 0)> ip 192.168.10.53 > 192.168.10.20 tcp 2054 > 80 PA 92df831b:b5812549(378)
@4310022559 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 A b5812549:92df8495(0)
@4310022559 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 A b5812549:92df8495(1448)
@4310022559 o( 1, 0)> ip 5.5.5.5 > 172.16.50.10 tcp 80 > 47234 PA a04040c:a9789345(1448)
@4310022559 i( 2, 1)> ip 192.168.10.20 > 192.168.10.53 tcp 80 > 2054 PA b5812af1:92df8495(1448)
```

Revision #1

Created 9 November 2022 14:18:20 by Mesut Bayrak

Updated 9 November 2022 14:18:32 by Mesut Bayrak